### Preserving Exchange Tasks (or Contacts or Calendars) from

Archive or Deletion Policies

Tasks, Calendars, and Contacts may be archived or deleted based on their calculated retention date, see <u>https://learn.microsoft.com/en-us/exchange/security-and-compliance/messaging-records-management/</u><u>retention-age?source=recommendations</u>

Unfortunately it's not always possible to create a policy on a folder that prevents archiving or deleting using retention policies or Outlook. So Microsoft has a crazy workaround for this (last tested May 2024).

Outlined steps below to set a retention policy on Tasks folder. First create the personal retention policy to stop archiving. We need to get the PR\_ARCHIVE\_TAG (step needs to be added).

1.Install EWS editor https://github.com/dseph/EwsEditor/releases

# EWSEditor - 1.24.0 Latest

You can now set the Authority and Scope in the log and other tenants.

▼ Assets 3

EwsEditor.1.24.-.bin.zip

Source code (zip)

Source code (tar.gz)

2. When you have it on your PC, it looks like this:

💱 EW	/SEditor 1	1.24.0.196	51			_	×
File	View	Tools	Other	Help			
					Name		Known
							Þ

Then, click on the File and choose New Exchange Service:



Use Autodiscover or use Exchange Web Service URL directly: O Autodiscover Email: Target mailbox. Example: myuser@contoso.com Service URL: https://outlook.office365.com/EWS/Exchange.as Example: https://mail.contoso.com/EWS/Exchange.asmx Note: For Autodiscover against out of network servers such as Exchange Online, you should set disable SCP Autodiscover so that only POX will be used. You can	Check if using EWS Id Type: SmtpAddress V Id: Set to mailbox being accessed for I
EWS Schema         Exchange2016           Set the version of the EWS Schema to use.         This is not the same thing as the Exch	SMTP: Normaly set to the target mailbox w
<ul> <li>Use Default Credentails</li> <li>Use the following oredentials instead of the default Windows credentials.</li> <li>User: Default Password: Default Password:</li> <li>Suggestion: Use UPN/SMTP address and no domain for Outlook 365.</li> <li>Use oAuth 2.0 (MSAL) (Registration must have been completed first)</li> <li>Select Authentication Flow</li> <li>Delegated Application</li> <li>Client App ID Tenant ID: Client Secret</li> <li>Authority: https://login.microsoftonline.com V Validate Authori</li> <li>Scope: https://outlook.office365.com/EWS.AccessAsUser.All V</li> </ul>	Set X-PublicFolderMailbox header SMTP: Set when accessing a public folder. Options Note: For delegate access: Log in as delegate then the tree menu select "A Root Folder". Use one of the opti to add the folder of the mailbox to the Note: The X-AnchorMailbox header shou always be set when EWS Impersonation Delegate Access are used. Calls may at any time if its not set.
	OK Car

3. login <u>App registrations - Microsoft Entra admin center</u>

## entra.microsoft.com/#view/Microsoft\_AAD\_RegisteredApps/CreateApplicationBlac

м	icrosoft Entra admin center		
<b>^</b>	Home What's new	Ă	Home > App registrations > Test_for_EWS > App registrations > Register an application
×	Diagnose & solve problems		* Name
*	Favorites	$\sim$	The user-facing display name for this application (this can be changed later).
۵	Identity	~	
i	Overview		Supported account types
8	Users	$\sim$	<ul> <li>Who can use this application or access this API?</li> <li>Accounts in this organizational directory only (Contoso only - Single tension)</li> </ul>
<b>የ</b> ድ	Groups	$\sim$	Accounts in any organizational directory (Any Microsoft Entra ID tenant
Ð	Devices	$\sim$	Xbox)
₿	Applications	~	Personal Microsoft accounts only
	Enterprise applications		Help me choose
Ī	App registrations		Redirect URI (optional)
ĉ	Roles & admins	$\sim$	We'll return the authentication response to this URI after successfully authent changed later, but a value is required for most authentication scenarios.
Ē	Billing	$\sim$	Public client/native (mobile V https://login.microsoftonline.com/co
0	Settings	$\sim$	
A	Protection	$\sim$	

Then, we can use the App's client ID and your tenant ID to sign-in;

←

С

ጨ

//Application ID is the client ID, and Directory ID is the tenant ID;

//please make sure the redirect URL is the one we just paste in the above picture;

#### ∧ Essentials

Display name	;	Test for EWS
Application (client) ID	;	cdbe888b-de5c-40de-a775-dcc0109d7080
Object ID	;	736368c3-df4c-483f-b6a4-4b11c6d9eb03
Directory (tenant) ID	:	eb106505-c67c-4c49-9a1f-631dd4414ce4
Supported account types	:	My organization only

## 4.Add API permission

м	icrosoft Entra admin center			${\cal P}$ Search resources, services, and	docs (G+/)	
\$	Home	Î	Ho	test for EWS > App registratio	ns > test for EWS > : ermissions	Request API permiss
**	What's new					Select an API
×	Diagnose & solve problems		2	Search «	🖒 Refresh 🛛 💆	Microsoft APIs APIs my organi
*	Favorites	$\sim$	N.	Overview		Apps in your directory that expose Al
	Identity		*	Integration assistant	Granting tenan their own beha	♥ office 365
(i)	Overview		Ma	anage	A The "Admin co	Office 365 Enterprise Insights
8	Users	$\sim$		Branding & properties	may not reflect	Office 365 Exchange Online
A-R	Crouns		<del>ک</del>	Authentication	Configurad parm	Office 365 Information Protection
×	Groups	Ť		Certificates & secrets	Applications are with	Office 365 Management APIs
20	Devices	$\sim$		Token configuration	include all the permis	Office 365 Search Service
₿	Applications	~	<del>.</del> - ව-	API permissions		Office 365 SharePoint Online
			<u>_</u>	Expose an API		
	Enterprise applications		8	App roles	API / Permissions r	
	App registrations		24	Owners	→ Microsoft Graph (	
A	Protection	$\sim$	2	Roles and administrators	User.Read	
			-()	Manifest	∨ Office 365 Exchan	

## **Request API permissions**

#### All APIs

Office 365 Exchange Online

https://outlook.office.com

What type of permissions does your application require?

#### Delegated permissions

Your application needs to access the API as the signed-in user.

#### Application permissions

Your application runs as a background service or daemon wi signed-in user.

Permission	Admin consent required
> Calendars	
> Contacts	
> EAS	
✓ EWS (1)	
EWS.AccessAsUser.All O Access mailboxes as the signed-in user via Exchange Web Services	No
> Exchange	



5.Login EWS editor

EWSEditor 1.24.0.19651 - Service	
Use Autodiscover or use Exchange Web Service URL directly: Autodiscover Email: Target mailbox. Example: myuser@contoso.com Service URL: https://outlook.office365.com/EWS/Exchange.as Example: https://mail.contoso.com/EWS/Exchange.asmx	Check if using EWS Id Type: SmtpAddress Id: Set to mailbox being accessed for I
Note: For Autodiscover against out of network servers such as Exchange Online, you should set disable SCP Autodiscover so that only POX will be used. You can	Set X-AnchorMailox header.
EWS Schema Exchange2016 V Set the version of the EWS Schema to use. This is not the same thing as the Excha	SMTP: Normaly set to the target mailbox w Impersonation and when accessing a
<ul> <li>Use Default Credentails</li> <li>Use the following oredentials instead of the default Windows oredentials.</li> <li>User: Default Password: Default Password: Suggestion: Use UPN/SMTP address and no domain for Outlook 365.</li> <li>Use oAuth 2.0 (MSAL) (Registration must have been completed first)</li> <li>Select Authentication Flow</li> <li>Delegated Application</li> <li>Client App ID cdbe888b-de5c-40de-a775-dcc0109d7080</li> <li>Tenant ID: eb106505-c67c-4c49-9a1f-631dd4414ce4</li> <li>Client Secret</li> <li>Authority: https://login.microsoftonline.com V Validate Authori</li> <li>Scope: https://outlook.office365.com/EWS.AccessAsUser.All</li> </ul>	Set X-PublicFolderMailbox header SMIP: Set when accessing a public folder. Options Note: For delegate access: Log in as delegate then the tree menu select "i Root Folder". Use one of the opti to add the folder of the mailbox to t Note: The X-AnchorMailbox header show always be set when EWS Impersonation Delegate Access are used. Calls may at any time if its not set.
hedirect URL: https://login.microsoftonline.com/common/oauth2/nativeclient	OK Car

Then, after you finish the authentication, please scroll down to find here:



first one is tag id

💀 Folder Archive Settings	—	
Note that GUID for PR_ARCHIVE_T	AG is created/obtained through the Exchange console or by PowerShell by an Administrator.	
See: <u>https://blogs.technet.mic</u> https://msdn.microsoft.co	rrosoft.com/anya/2014/11/19/understanding-of-managed-folder-assistant-with-retention-policies/ m/en-us/library/ee202166(v=exchg.80).aspx	•
<u>https://blogs.msdn.micros</u> https://blogs.technet.mic	soft.com/akashb/2012/12/07/stamping-archive-policy-tag-using-ews-managed-api-from-powershellex prosoft.com/surama/2011/10/19/search-and-replace-retention-tag-on-microsoft-exchange-2010-mrm/	<u>change=201</u>
PR_ARCHIVE_TAG (0x3018):	a4b7f232-d3e0-47d7-af44-a150f0b0f610	
<pre>FR_RETENTION_FLAGS (0x301D):</pre>	16Bitmask value.0x0010 = ExplictArchiveTag (0x0010).	
PR_ARCHIVE_PERIOD (0x301E):	0 This is the number of days. O or -1 means never expire.	
Note: When PR_RETENTION_FLAGS :	is set, Exchange may update its bitmask include the next action to perform — such as NeedsReso	an and Per
		Can

If you want to use delegation instead

0

if you want to use delegated permissions from the admin account rather than authenticating as the user (which could require working with them to allow MFA, etc) is to right click over the admin account that gets added and add a folder:

🔆 EWSEditor 1.24.0.19651 - EWSEditor - Select a Folderld
O Identify folder by unique id.
Unique ID
Folder Id:
Identify folder by well known name.
Well Known Folder Name
Folder Name: Root ~
SMTP address for the mailbox to do delegate access to:
SMTP Address: mzachcoki@amfiberservices.com
Enter the SMTP address of the mailbox to access using delegate access. Leave this field empty to access the default mailbox.
O Identify folder by well known name.
Pick Folder
Pick Folder Id:
OK Cancel

Then you can see the user's mailbox and go to Top Of Information Store->Tasks to apply the policies.



In addition - I found another workaround for this problem that, at least temporarily, takes care of both the archive and deletion issues, but is also less than ideal and requires some finagling. Basically, I can export the Tasks to a CSV file, then delete them, and re-import them, which creates them "as new" with a new creation date. It is a little finicky, and it doesn't work so well for recurring tasks, but then again those are the ones that aren't a problem in the first place, since when a user marks it complete, it generates a new task with a new creation date. This method does mean the archival/deletion will still occur, but now it will occur years in the future (or whenever the retention policy says).